แผนบริหารความเสี่ยง
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
โรงเรียนการบิน
พ.ศ.๒๕๖๙

สารบัญ

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารโรงเรียนการบิน
พ.ศ.๒๕๖๙

๑. หลักการและเหตุผล

ปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสาร เทคโนโลยีปัญญาประดิษฐ์ (AI) ที่เข้ามาเป็นปัจจัยสำคัญในการปฏิบัติงานของ ทอ.เพื่อเสริมสร้างกำลังทางอากาศไปสู่กองทัพอากาศที่แข็งแกร่งและมีประสิทธิภาพให้ได้ (Strengthening Air Power towards Unbeatable Air Force) จะเกิดขึ้นได้ ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ทอ. ต้องมั่นคงปลอดภัย (Security) พร้อมใช้งาน (Availability) และความถูกต้องสมบูรณ์ของข้อมูล (Integrity) การบริหารจัดการความเสี่ยง มีบทบาทสำคัญในการปกป้องข้อมูลและระบบเครือข่ายคอมพิวเตอร์ที่เป็นทรัพย์สินของหน่วยงาน และยังรวมถึงการปกป้อง "ภารกิจ" ของหน่วยงานให้รอดพ้นจากความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารอีกด้วย

ขั้นตอนในการบริหารจัดการความเสี่ยง ควรจัดให้อยู่ในความรับผิดชอบหลักของหน่วย ซึ่งมีผู้เชี่ยวชาญในด้านเทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้บังคับบัญชา และผู้ดูแลระบบของหน่วยงานจะต้องมีกระบวนการในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เหมาะสมและได้มาตรฐาน เพื่อปกป้องหน่วยงานจากความเสียหายที่อาจเกิดขึ้นได้จากความเสี่ยง และเพื่อความสามารถในการดำเนินภารกิจของหน่วยให้บรรลุผลสำเร็จ ไม่ใช่แค่เพียงการปกป้องสินทรัพย์เทคโนโลยีสารสนเทศหรือหน่วยงานเพียงเท่านั้น

การบริหารความเสี่ยงมีความสำคัญต่อการบริหารราชการแบบมุ่งผลสัมฤทธิ์ตามพระราชกฤษฎีกาว่าด้วยการบริหารกิจการบ้านเมืองที่ดี พ.ศ.๒๕๔๖ เนื่องจากการบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการบริหารกลยุทธ์ เป็นการเพิ่มโอกาสและช่วยให้หน่วยงานบรรลุเป้าประสงค์และภารกิจที่ตั้งไว้ และเป็นการพัฒนาผลการปฏิบัติงานของหน่วยงาน ที่จะนำไปสู่การใช้ทรัพยากรอย่างมีประสิทธิภาพและคุ้มค่า

๒. วัตถุประสงค์

๒.๑ เพื่อให้การบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารภายใน รร.การบิน ดำเนินการได้อย่างมีประสิทธิภาพ มีความยืดหยุ่นสามารถปรับตัวได้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศและการสื่อสารสมัยใหม่ ภายใต้ข้อจำกัดที่บุคลากรด้านเทคโนโลยีสารสนเทศและการสื่อสารของ รร.การบินมีจำนวนจำกัด และลดโอกาสในการเกิดความเสียหาย หรือความผิดพลาดกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของ รร.การบิน

๒.๒ เพื่อเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉิน ภัยคุกคาม ความผิดพลาด ความไม่พร้อมใช้งานหรือเหตุที่ไม่พึงประสงค์ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของ รร.การบิน

๒.๓ เพื่อให้มีการวางแผนการปฏิบัติ การควบคุม และกำหนดแนวทางแก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๔ เพื่อเป็นแนวทางการดำเนินการ การกำกับดูแล การตรวจสอบเกี่ยวกับการบริหารจัดการและการเผยแพร่ความรู้ ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๕ เพื่อเพิ่มประสิทธิภาพในการพิจารณาดำเนินการของผู้รับผิดชอบระบบเทคโนโลยีสารสนเทศและการสื่อสารของ รร.การบิน โดยคำนึงถึงปัจจัยเสี่ยง และความเสี่ยงในด้านต่าง ๆ ที่อาจส่งผลกระทบกับการดำเนินงานตามวัตถุประสงค์และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงหรือผลกระทบที่อาจเกิดขึ้น ก่อนตัดสินใจในการดำเนินการหรือปฏิบัติตามแผนอย่างใดอย่างหนึ่ง

๓. ระเบียบ...

๓. ระเบียบ และแผนปฏิบัติที่เกี่ยวข้อง

๓.๑ คู่มือการจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทอ.พ.ศ.๒๕๖๒

๓.๒ ระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓

๓.๓ แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทสส.ทอ.พ.ศ.๒๕๖๔

๓.๔ ระเบียบ รร.การบิน ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๕

๔. ขอบเขตการดำเนินการ

เป็นแผนบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารภายใน รร.การบิน โดยกำหนดแนวทางปฏิบัติให้กับผู้รับผิดชอบระบบสารสนเทศและการสื่อสาร รวมทั้งบุคลากร คอมพิวเตอร์ และอุปกรณ์เครือข่าย พร้อมกับการสร้างจิตสำนึก และความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีคณะกรรมการรักษาความปลอดภัยระบบสารสนเทศของ ทสส.ทอ.เป็นผู้รับผิดชอบหลักในการกำหนดแผนบริหารจัดการความเสี่ยง

๕. การประเมินโอกาสหรือความน่าจะเป็นของเหตุการณ์ที่อาจเกิดขึ้น

การประเมินโอกาสหรือความน่าจะเป็นของเหตุการณ์ที่อาจเกิดขึ้น (Probability or Likelihood) กับระบบเทคโนโลยีสารสนเทศและการสื่อสาร รร.การบิน ตามแผนบริหารความเสี่ยงฯ นี้ พิจารณาแบ่งความถี่ของโอกาสหรือความน่าจะเป็นของเหตุการณ์ที่อาจเกิดขึ้นเป็น ๕ ระดับ จากน้อยไปหามาก ดังนี้

ระดับ	โอกาสที่เกิดขึ้น
๑	แทบไม่เกิดขึ้นเลย (Improbable)
๒	น้อยครั้งมาก (Remote)
๓	ตามโอกาส (Occasional)
๔	ประปราย (Probable)
๕	เกิดขึ้นบ่อย (Frequent)

การประเมินผลกระทบหรือความรุนแรงของเหตุการณ์ (Severity of consequence) แบ่งระดับผลกระทบหรือความรุนแรงเป็น ๕ ระดับ จากน้อยไปหามาก ดังนี้

ระดับ	ผลกระทบ/ความรุนแรง
๑	น้อยมาก - เกิดเหตุร้ายที่ไม่มีความสำคัญ
๒	น้อย - เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
๓	ปานกลาง - ระบบมีปัญหา และมีความสูญเสียไม่มาก
๔	สูง - เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
๕	สูงมาก - เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่าง ๆ

๖. การประเมินค่าความเสี่ยง

พิจารณาจากปัจจัยของโอกาสหรือความน่าจะเป็นของเหตุการณ์ กับระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร รร.การบิน รวมถึงประสิทธิภาพของแผนการควบคุมความปลอดภัย การวัดระดับความเสี่ยงพิจารณาจากแผนภูมิความเสี่ยงกับผลกระทบที่เกิดขึ้นและขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

ระดับ...

ระดับความเสี่ยง = โอกาสที่จะเกิดขึ้นของเหตุการณ์ x ผลกระทบความรุนแรงของเหตุการณ์

แผนผังประเมินความเสี่ยง (ระดับความเสี่ยง)

ผลกระทบ					
๕	๑๐	๑๕	๒๐	๒๕
๔	๘	๑๒	๑๖	๒๐
๓	๖	๙	๑๒	๑๕
๒	๔	๖	๘	๑๐
๑	๒	๓	๔	๕
		โอกาส		

ค่าความเสี่ยง	ระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
๑ - ๘	ต่ำ	ยอมรับความเสี่ยง	ขาว
๙ - ๑๖	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง
๑๗ - ๒๔	สูง	ควบคุมความเสี่ยง (มีแผนควบคุม)	ฟ้า
๒๕	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

๖.๑ การยอมรับความเสี่ยง (Risk Acceptance) คือ การยอมรับความเสี่ยงในระดับที่เป็นอยู่และให้ระบบข้อมูลสารสนเทศดำเนินการไปตามปกติ ซึ่งเป็นการยอมรับในผลที่อาจตามมา เช่น การพิสูจน์ตัวตนเพียงใช้ชื่อผู้ใช้งาน และรหัสผ่านมีความเสี่ยงเพราะอาจมีการขโมยไปใช้ได้ การใช้ Biometrics เช่น การตรวจลายนิ้วมือหรือม่านตา อาจมีค่าใช้จ่ายสูงไม่คุ้มค่า หน่วยงานอาจยอมรับความเสี่ยงของระบบปัจจุบัน โดยทำงานต่อไป และปรับปรุงเมื่อมีโอกาส

๖.๒ การจำกัดความเสี่ยง (Risk Limitation) คือ การทำระบบควบคุมเพื่อให้เกิดผลกระทบจากการถูกคุกคามระบบหรือจากความไม่มั่นคงของระบบให้น้อยที่สุด เช่น การใช้ Firewall ป้องกันระบบจากภัยคุกคามในอินเทอร์เน็ต

๖.๓ การควบคุมความเสี่ยง (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ ๔ ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

๖.๔ การถ่ายโอนความเสี่ยง (Risk Transfer) คือ การถ่ายโอนความเสี่ยงด้วยการหาทางเลือกอื่นเพื่อชดเชยความสูญเสีย เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน หน่วยงานอาจเลือกซื้อประกัน หรือสัญญาการซ่อมบำรุง เป็นต้น

๗. การวิเคราะห์ความเสี่ยง ลักษณะ และรายละเอียดของความเสี่ยง

๗.๑ การวิเคราะห์ความเสี่ยง จากการวิเคราะห์ และพิจารณาความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ รร.การบิน สามารถแยกประเภทความเสี่ยงได้เป็น ๔ ประเภท ดังนี้

๗.๑.๑ ความเสี่ยงด้านเทคนิค (Risk of technical : RT) เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์อาจเกิดถูกโจมตีจากไวรัสหรือโปแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

๗.๑.๒ ความเสี่ยง...

๗.๑.๒ ความเสี่ยงจากผู้ปฏิบัติงาน (Risk of people : RP) เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่าง ๆ ของหน่วยงานเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

๗.๑.๓ ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน (Risk of disaster or emergency situation : RE) เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๗.๑.๔ ความเสี่ยงด้านการบริหารจัดการ (Risk of management : RM) เป็นความเสี่ยงจากนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศและการสื่อสารของ รร.การบิน หรือจากนโยบายในระดับที่สูงกว่าที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศของโรงเรียนการบิน

๗.๒ ลักษณะและรายละเอียดของความเสี่ยง (Description of risk)

ลักษณะและรายละเอียดของความเสี่ยงของระบบเทคโนโลยีสารสนเทศและการสื่อสารของ รร.การบิน ที่ได้จากการร่วมกันวิเคราะห์ และระดมความคิดของผู้รับผิดชอบระบบเทคโนโลยีสารสนเทศ รวมถึงเหตุการณ์ที่ รร.การบิน เผชิญ (ตามแนวทางการระบุความเสี่ยง) แสดงตามตาราง

ตารางแสดงลักษณะและรายละเอียดของความเสี่ยง (Description of risk)

รหัสความเสี่ยง	ชื่อความเสี่ยง (เหตุการณ์)	ลักษณะ	ปัจจัยเสี่ยง (สาเหตุ)	ผลกระทบ	โอกาส	ความรุนแรง	ค่าความเสี่ยง
RP01	การเข้าถึงข้อมูลของบุคคลอื่น	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	- การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล/เปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต	- ผู้ใช้งาน - ระบบสารสนเทศ - ระบบฐานข้อมูล	๓	๕	๑๕
RP02	การนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ Wireless router หรือ Switch/Hub มาเชื่อมต่อกับระบบเครือข่ายหน่วยงาน โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์ในระบบเครือข่ายไม่สามารถ ใช้งานได้ หรือการไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกรับสัญญาณได้และเชื่อมต่อเข้ากับระบบเครือข่ายของหน่วยงาน ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัยของหน่วยงาน	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ - ความล้มเหลวทางเทคนิค	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	๔	๔	๑๖

รหัสความเสี่ยง	ชื่อความเสี่ยง (เหตุการณ์)	ลักษณะ	ปัจจัยเสี่ยง (สาเหตุ)	ผลกระทบ	โอกาส	ความรุนแรง	ค่าความเสี่ยง
RP03	ภัย Social Engineering และการหลอกลวงโดยการทำ phishing	- การหลอกลวงทางจิตวิทยาที่มุ่งเป้าไปที่การโจรกรรมข้อมูลส่วนบุคคลหรือข้อมูลทางการเงิน โดยหลอกให้เป้าหมายเป็นผู้ให้ข้อมูลนั่นเอง การกลั่นแกล้งบนโลกไซเบอร์เป็นการทำร้ายกันทางความรู้สึกหรือจิตใจ เช่น การโพสต์ข้อความ ภาพหรือคลิปวิดีโอเพื่อส่อเสียด ประจาน โจมตี ข่มขู่ หรือใช้ถ้อยคำหยาบคาย ทำให้เหยื่อเกิดความอับอาย เสื่อมเสียชื่อเสียง แพร่กระจายออกไปอย่างกว้างขวางและรวดเร็ว	- กำลังพลอาจถูกหลอกลวงได้หลายวิธี เช่น การทำ อีเมล์ Phishing การโทรศัพท์หลอกลวงเพื่อถามข้อมูล หรือให้ทำธุรกรรมทางการเงิน - การโพสต์ระบายสิ่งที่ไม่พอใจต่อเพื่อนร่วมงาน หัวหน้างาน องค์กร หรือเกี่ยวข้องกับ ๓ สถาบันหลัก เป็นต้น	- ทำให้สูญเสียข้อมูลส่วนบุคคลที่สำคัญ ซึ่งอาจนำไปสู่การเป็นคดีความ - อาจทำให้สูญเสียทรัพย์สินจากการขโมยทำธุรกรรมทางการเงิน - ผู้ได้รับผลกระทบคือ กำลังพล - การโพสต์ทำให้เหยื่อเกิดความอับอาย หรือเสื่อมเสียชื่อเสียง	๕	๕	๒๕
RP04	นำข้อมูลของทางราชการไปใช้กับเทคโนโลยีปัญญาประดิษฐ์ (AI)	- การใช้ AI (เช่น Generative AI หรือ Chatbot) สรุปรายงานราชการที่มีชั้นความลับ	- งานราชการมีเอกสารรายงานที่หนาและซับซ้อนจำนวนมาก ข้าราชการเผชิญความกดดันเรื่องเวลา จึงเลือกใช้ AI เป็นทางลัดเพื่อความรวดเร็ว โดยอาจไม่ได้ตระหนักถึงเรื่องความปลอดภัย (เกิดพฤติกรรม Shadow IT หรือการแอบใช้เครื่องมือนอกระบบ)	- ข้อมูลรั่วไหลภายนอก (Data Leakage): ข้อมูลลับจะหลุดออกจากเครือข่ายรัฐทันทีเมื่อ Upload และไปบันทึกอยู่บนเซิร์ฟเวอร์ภายนอก (Cloud) ซึ่งมักตั้งอยู่ในต่างประเทศ - ข้อมูลถูกนำไปเทรน AI (Data Re-use): ผู้ให้บริการ AI (โดยเฉพาะเวอร์ชันฟรี) สามารถนำข้อมูลลับที่ป้อนไปใช้พัฒนาโมเดล ส่งผลให้ข้อมูลนั้นอาจหลุดไปเป็นคำตอบให้กับผู้ใช้งานคนอื่นได้ - การถูกจารกรรมไซเบอร์ (Cyber Espionage): หากบัญชีผู้ใช้ของเจ้าหน้าที่ถูกแฮก	๒	๓	๖

รหัสความเสี่ยง	ชื่อความเสี่ยง (เหตุการณ์)	ลักษณะ	ปัจจัยเสี่ยง (สาเหตุ)	ผลกระทบ	โอกาส	ความรุนแรง	ค่าความเสี่ยง
				แฮกเกอร์จะสามารถเข้าถึงประวัติการแชทและอ่านเนื้อหาเอกสารลับทั้งหมดที่เคยสั่งให้ AI สรุปได้ทันที			
RT01	การถูกไวรัสหรือโปรแกรมประสงค์ร้ายเข้าทำลายหรือขโมยข้อมูล	คอมพิวเตอร์หรือระบบเครือข่ายถูกเจาะเข้ามาโดย Hacker ที่อาจเป็นบุคคลภายในหรือภายนอก รร.การบิน เพื่อทำลายหรือขโมยข้อมูล	- เครื่องคอมพิวเตอร์ไม่ได้เปิดใช้งาน firewall หรือ ไม่ได้ติดตั้ง Antivirus - การแชร์โฟลเดอร์โดยไม่ใส่รหัส - ระบบปฏิบัติการหรือโปรแกรมมีช่องโหว่	-ทำให้ข้อมูลสำคัญเสียหายหรือถูกขโมยไปใช้ประโยชน์ และอาจเกิดการแพร่กระจายไวรัส -ผู้ได้รับผลกระทบ คือ ผู้ใช้งานและระบบสารสนเทศ รร.การบิน	๕	๕	๒๕
RT02	การใช้ BYOD /Mobile Devices ใน รร.การบิน	- การนำอุปกรณ์ส่วนตัว เช่น คอมพิวเตอร์และโทรศัพท์มือถือ เข้ามาเชื่อมต่อกับเครือข่าย ทอ. หรือเครือข่ายภายใน รร.การบิน อาจกลายเป็นช่องโหว่ให้เกิดการโจมตีจากผู้ประสงค์ร้ายและการขโมยข้อมูล	- คอมพิวเตอร์ส่วนตัวและโทรศัพท์มือถือสามารถเชื่อมต่อกับเครือข่ายอื่นในสถานที่ที่อาจไม่ได้รักษาความปลอดภัย จึงมีโอกาสที่ข้อมูลสำคัญของราชการและข้อมูลส่วนตัวถูกขโมยออกไปได้ง่าย - แอพลิเคชันบนโทรศัพท์มือถือมักจะขอสิทธิ์การเข้าใช้หรือเข้าถึงข้อมูลบนโทรศัพท์และนำข้อมูลนั้นไปใช้ประโยชน์	- ทำให้ข้อมูลส่วนตัวและข้อมูลสำคัญของทางราชการอาจรั่วไหลได้ -ผู้ได้รับผลกระทบ คือ ผู้ใช้งาน และ รร.การบิน	๔	๕	๒๐
RT03	เครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะ เช่น หนูหรือแมลง	- การไม่ทำความสะอาดสถานที่ตั้งอุปกรณ์คอมพิวเตอร์และเครือข่าย - บริเวณรอบสถานที่ตั้งอุปกรณ์มีหญ้าขึ้นรก สภาพสกปรก ทำให้หนู แมลงหรือสัตว์ เข้ามาอาศัย	- ทำให้อุปกรณ์คอมพิวเตอร์ได้รับความเสียหาย - ผู้ได้รับผลกระทบ คือ ผู้ใช้งาน	๔	๕	๒๐

รหัสความเสี่ยง	ชื่อความเสี่ยง (เหตุการณ์)	ลักษณะ	ปัจจัยเสี่ยง (สาเหตุ)	ผลกระทบ	โอกาส	ความรุนแรง	ค่าความเสี่ยง
RT04	การขาดแคนเครื่องคอมพิวเตอร์สำหรับการปฏิบัติงาน	เครื่องคอมพิวเตอร์ ชำรุดไม่สามารถซ่อมแซม หรือทดแทนได้	- เนื่องจากเครื่องคอมพิวเตอร์ไม่มีเลขพัสดุ - ได้รับการแจกจ่ายเครื่องคอมพิวเตอร์มาไม่เพียงพอกับความต้องการ	- ทำให้ไม่สามารถจัดหาคอมพิวเตอร์ให้กำลังพลใช้งานได้อย่างเหมาะสม - กำลังพลดำเนินการจัดซื้อเครื่องคอมพิวเตอร์มือสองที่มีทรัพยากรไม่เพียงพอ ระบบปฏิบัติการต่ำมาใช้งานทำให้ไม่สามารถลงโปรแกรมป้องกันไวรัสได้	๔	๕	๒๐
RT05	ระบบปฏิบัติการของเครื่องคอมพิวเตอร์ไม่สามารถอัพเดทได้	- เครื่องคอมพิวเตอร์มีอายุการใช้งานที่ยาวนาน สภาพเก่าโดยส่วนมากที่พบจะเป็นระบบปฏิบัติการ Windows 7 ซึ่งไม่สามารถอัพเดทแพทหรือลงระบบปฏิบัติการใหม่ได้แล้ว	- เกิดช่องโหว่ที่รุนแรง EternalBlue (MS17-010) ที่ใช้โจมตีผ่านเครือข่าย และช่องโหว่ประเภท Privilege Escalation (การยกระดับสิทธิ์)	- แฮกเกอร์ใช้กระจาย Malware เรียกค่าไถ่ (Ransomware) อย่าง WannaCry - ช่องโหว่ที่อนุญาตให้โปรแกรมธรรมดาหรือผู้ใช้ระดับทั่วไป เจาะทะลุไปยึดสิทธิ์ระดับ Administrator ของเครื่อง ทำให้ควบคุมระบบได้ทั้งหมด	๓	๕	๑๕
RT06	การถูกโจมตีทางไซเบอร์จากสถานการณ์ความตึงเครียดบริเวณชายแดนไทย-กัมพูชา	- เจาะระบบจารกรรม (Espionage): แฮกเกอร์ค้นหาช่องโหว่ระบบเพื่อขโมยข้อมูลกำลังพล แผนผังยุทธการ หรือดักจับบัญชีอีเมลทหาร - หลอกลวงจิตวิทยา (Phishing) ส่งอีเมลหรือเอกสารราชการปลอม (Spear-Phishing) เพื่อหลอกให้เจ้าหน้าที่คลิกลิงก์อันตรายหรือฝัง Malware	- มิติด้านภูมิรัฐศาสตร์ (Geopolitics) สถานการณ์ความตึงเครียดตามแนวชายแดน หรือความขัดแย้งระหว่างประเทศ เป็นตัวกระตุ้นให้กลุ่มแฮกเกอร์ข้ามชาติ (APT) และกลุ่มแฮกเกอร์ชาตินิยม (Hacktivist) พุ่งเป้าโจมตี ทอ.เป็นอันดับแรก - มิติด้านเทคโนโลยีและโครงสร้างพื้นฐาน: ระบบบางส่วนของ ทอ.	- ระบบงานหยุดชะงัก: การโจมตีไซเบอร์ (เช่น DDoS หรือเจาะระบบ) ทำให้เว็บไซต์ ช่องทางสื่อสาร หรือระบบบริการภายในล่ม จนใช้งานไม่ได้ในสถานการณ์วิกฤต - ดิสเครดิตกองทัพ การที่หน้าเว็บถูกเปลี่ยนแปลง (Defacement) หรือมีข้อมูลรั่วไหล	๒	๕	๑๐

รหัสความเสี่ยง	ชื่อความเสี่ยง (เหตุการณ์)	ลักษณะ	ปัจจัยเสี่ยง (สาเหตุ)	ผลกระทบ	โอกาส	ความรุนแรง	ค่าความเสี่ยง
		- ยิงระบบล่ม (DDoS): ระดมส่งทราฟฟิกมหาศาลถล่มเว็บไซต์ ทอ.ให้ใช้งานไม่ได้ เพื่อผลทางจิตวิทยาและดิสเครดิตองค์กร	โดยเฉพาะเว็บแอปพลิเคชันย่อย ขาดการอัปเดตระบบความปลอดภัย (Patching) อย่างสม่ำเสมอ หรือขาดการตั้งค่าระบบยืนยันตัวตนหลายชั้น (MFA) ทำให้มีช่องโหว่ให้เจาะเข้ามาได้ง่าย	สู่สาธารณะ จะลดทอนความเชื่อมั่นของประชาชนที่มีต่อศักยภาพในการป้องกันประเทศของ ทอ.			
RT07	การเชื่อมต่อระหว่างเครือข่ายภายนอกและเครือข่ายภายในไม่มีการรักษาความปลอดภัยผ่านระบบ NAC และ Firewall	เครื่องคอมพิวเตอร์เชื่อมต่อเครือข่ายภายนอกและถูกโจมตีโดยการติดตั้ง Malware ฝังไว้กับตัวเครื่อง เมื่อเครื่องคอมพิวเตอร์สลับกลับมาใช้เครือข่ายภายใน Malware ก็จะทำการแพร่กระจายไปยังเครื่องอื่นภายในเครือข่ายโดยที่ไม่ผ่านการตรวจจับจากระบบ NAC และ Firewall	- ผู้ใช้งานเครื่องคอมพิวเตอร์ที่เชื่อมต่อเครือข่ายภายนอก อาจมีพฤติกรรมการใช้งานอินเทอร์เน็ตที่มีความเสี่ยง เช่น การเข้าเว็บไซต์อโคจร การดาวน์โหลดโปรแกรมไม่ถูกลิขสิทธิ์ การคลิกเว็บไซต์โฆษณาที่มี Malware - ผู้ใช้งานไม่ติดตั้งโปรแกรม Antivirus หรือ โปรแกรม Antivirus ไม่ update ไม่สามารถป้องกัน Malware ได้ - ผู้ใช้นำเครื่องคอมพิวเตอร์ที่ติด Malware มาเชื่อมต่อกับเครือข่ายภายใน ทอ. และใช้งานระบบที่สำคัญภายใน ทอ.	- Malware กระจ่ายเข้าสู่ระบบเครือข่ายภายใน ทอ. - Hacker สามารถโจมตีระบบสารสนเทศที่สำคัญของ ทอ. ทำให้ไม่สามารถใช้งานได้ - Username และ Password ในระบบข้อมูลของ ทอ.ที่มีชั้นความลับอาจรั่วไหล	๔	๕	๒๐
RM01	การขาดแคลนบุคลากรผู้ปฏิบัติงาน	การขาดแคลนบุคลากรด้านสารสนเทศทำให้การทำงานอาจหยุดชะงักหากบุคลากรไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	- จนท.สารสนเทศ รร.การบินมีไม่เพียงพอ - จนท.สารสนเทศที่แต่งตั้งขึ้นประจำหน่วยใน รร.การบินขาดความรู้และขาดทักษะในการดูแลเครือข่ายและอุปกรณ์คอมพิวเตอร์ -	- ทำให้การบริหารจัดการทรัพยากรเครื่องคอมพิวเตอร์และระบบเครือข่ายไม่มีประสิทธิภาพ - ผู้ได้รับผลกระทบ คือ นทสส.รร.การบิน, นขต.รร.การบิน, จนท.สารสนเทศ นขต.รร.การบิน	๔	๓	๑๒

รหัสความเสี่ยง	ชื่อความเสี่ยง (เหตุการณ์)	ลักษณะ	ปัจจัยเสี่ยง (สาเหตุ)	ผลกระทบ	โอกาส	ความรุนแรง	ค่าความเสี่ยง
RM02	การเปลี่ยนแปลงนโยบายผู้บังคับบัญชา	การเปลี่ยนแปลงผู้บังคับบัญชา อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลง ทำให้การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	- ผู้บังคับบัญชาเปลี่ยนแผนการปฏิบัติงานกระทันหัน	- ทำให้การปฏิบัติงานของ จนท.เทคโนโลยีสารสนเทศไม่เป็นไปตามที่วางแผนไว้ ผู้ได้รับผลกระทบ คือ นทสส.ฯ จนท.สารสนเทศ นขต.รร.การบิน	๑	๑	๑
RM03	การได้รับงบประมาณสนับสนุนไม่เพียงพอ	การขาดแคลนงบประมาณในการดำเนินการ ทำให้ระบบสารสนเทศไม่สามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	- งบประมาณไม่เพียงพอต่อการจัดหาคอมพิวเตอร์ใหม่มาทดแทน หรือบำรุงรักษาซ่อมแซม	- ทำให้ไม่สามารถจัดหาอะไหล่ซ่อมบำรุงเครื่องคอมพิวเตอร์ - อุปกรณ์บางอย่างมีราคาสูง ไม่สามารถซ่อมแซมได้ -ผู้ได้รับผลกระทบ คือ ผู้ใช้งานและ จนท.สารสนเทศฯ	๔	๒	๘
RM04	การโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- เกิดการขโมยอะไหล่ชิ้นส่วนคอมพิวเตอร์เพื่อนำไปใช้หรือขาย	- ทำให้เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ - ผู้ได้รับผลกระทบ คือ ผู้ใช้งาน	๑	๕	๕
RE01	ระบบไฟฟ้าขัดข้องและไฟไหม้	คอมพิวเตอร์และระบบเครือข่ายเกิดการหยุดชะงัก เนื่องจากขาดระบบไฟฟ้า หรือเกิดเพลิงไหม้จนอุปกรณ์ได้รับความเสียหาย	- กระแสไฟฟ้าตก ไฟกระชาก หรือดับกระทันหัน - เกิดเพลิงไหม้จากกระแสไฟฟ้าลัดวงจร	- อุปกรณ์ภายในคอมพิวเตอร์อาจเสียหายจากกระแสไฟฟ้ากระชาก หรือดับกระทันหัน - ผู้ได้รับผลกระทบ คือ ผู้ใช้งาน และ รร.การบิน สูญเสียงบประมาณในการจัดหาใหม่ทดแทน	๓	๔	๑๒

๘. ผลการวิเคราะห์ความเสี่ยง (Risk reporting)

จากผลการระบุความเสี่ยงร่วมวิเคราะห์ และประเมินความเสี่ยงของผู้รับผิดชอบระบบเทคโนโลยีสารสนเทศ สามารถจัดลำดับความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ รร.การบิน เพื่อใช้ในการบริหารจัดการได้ดังนี้

๕	๑๐	๑๕	๒๐	๒๕
๔	๘	๑๒	๑๖	๒๐
๓	๖	๙	๑๒	๑๕
๒	๔	๖	๘	๑๐
๑	๒	๓	๔	๕

ตารางและลำดับผลการวิเคราะห์ความเสี่ยง (จากมากไปน้อย)

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๑	การถูกไวรัสหรือโปรแกรมประสงค์ร้ายเข้าทำลายหรือขโมยข้อมูล	เทคนิค RT01	- คอมพิวเตอร์หรือระบบเครือข่ายถูกเจาะเข้ามาโดย Hacker ที่อาจเป็นบุคคลภายในหรือภายนอก รร.การบิน เพื่อทำลายหรือขโมยข้อมูล	๒๕
๒	การหลอกลวงโดยการทำ phishing และ การกลั่นแกล้งรังแกบนโลกไซเบอร์ (Cyber bullying)	ผู้ปฏิบัติงาน RP03	- การหลอกลวงทางจิตวิทยาที่มุ่งเป้าไปที่การโจรกรรมข้อมูลส่วนบุคคล หรือข้อมูลทางการเงิน โดยหลอกให้เป้าหมายเป็นผู้บอก หรือให้ข้อมูลนั้นเอง - การกลั่นแกล้งรังแกบนโลกไซเบอร์ เป็นการทำร้ายกันทางความรู้สึกหรือจิตใจ เช่น การโพสต์ข้อความ ภาพ หรือคลิปวิดีโอเพื่อด่าทอ ส่อเสียด ประจาน แฉ โจมตี ข่มขู่ หรือใช้ถ้อยคำหยาบคาย ทำให้เหยื่อเกิดความอับอาย เสียใจ หรือเสื่อมเสียชื่อเสียง แพร่กระจายออกไปอย่างกว้างขวางและรวดเร็วเมื่อมีการส่งต่อ	๒๕
๓	การใช้ BYOD/Mobile Devices ใน รร.การบิน	เทคนิค RT02	- การนำอุปกรณ์ส่วนตัว เช่น คอมพิวเตอร์และโทรศัพท์มือถือเข้ามาเชื่อมต่อกับเครือข่าย ทอ. หรือเครือข่ายภายใน รร.การบิน อาจกลายเป็นช่องโหว่ให้เกิดการโจมตีจากผู้ประสงค์ร้ายและการขโมยข้อมูล	๒๐
๔	เครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	เทคนิค RT03	- เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	๒๐
๕	การขาดแคนเครื่องคอมพิวเตอร์สำหรับการปฏิบัติงาน	เทคนิค RT04	- เครื่องคอมพิวเตอร์ ชำรุด ไม่สามารถซ่อมแซม หรือขอทดแทนใหม่ได้	๒๐
๖	การเชื่อมต่อระหว่างเครือข่ายภายนอกและเครือข่ายภายในไม่มีการรักษาความปลอดภัยผ่านระบบ NAC และ Firewall	เทคนิค RT07	เครื่องคอมพิวเตอร์เชื่อมต่อเครือข่ายภายนอกและถูกโจมตีโดยการติดตั้ง Malware ฝังไว้กับตัวเครื่อง เมื่อเครื่องคอมพิวเตอร์สลับกลับมาใช้เครือข่ายภายใน Malware ก็จะทำการแพร่กระจายไปยังเครื่องอื่นภายในเครือข่ายโดยที่ ไม่ผ่านการตรวจจับจากระบบ NAC และ Firewall	๒๐

ลำดับ	ความเสี่ยง	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับความเสี่ยง
๗	การนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	ผู้ปฏิบัติ RP02	- ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำ wireless router หรือ switch/hub มาเชื่อมต่อกับระบบเครือข่ายหน่วยงาน โดยไม่ได้รับอนุญาต และ ← ไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ หรือ การไม่ได้ตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่น ๆ ที่รับสัญญาณได้ เชื่อมต่อเข้ากับระบบเครือข่ายของหน่วยงาน	๑๖
๘	การเข้าถึงข้อมูลของบุคคลอื่น	ผู้ปฏิบัติ RP01	- ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	๑๕
๙	ระบบปฏิบัติการของเครื่องคอมพิวเตอร์ไม่สามารถอัพเดทได้	เทคนิค RT05	เครื่องคอมพิวเตอร์มีอายุการใช้งานที่ยาวนานสภาพเก่าโดยส่วนมากที่พบจะเป็นระบบปฏิบัติการ Windows 7 ซึ่งไม่สามารถอัพเดทแพทหรือลงระบบปฏิบัติการใหม่ได้แล้ว	๑๕
๑๐	กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	เทคนิค/หรือสถานการณ์ฉุกเฉิน RE01	- การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือ เมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	๑๒
๑๑	การขาดแคลนบุคลากรผู้ปฏิบัติงาน	การบริหารจัดการ RM01	- การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ และจำนวนบุคลากรมีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	๑๒
๑๒	การถูกโจมตีทางไซเบอร์จากสถานการณ์ความตึงเครียดบริเวณชายแดนไทย-กัมพูชา	เทคนิค RT06	เจาะระบบจารกรรม (Espionage): แฮกเกอร์ค้นหาช่องโหว่ระบบเพื่อขโมยข้อมูลกำลังพล แผนผังยุทธการ หรือดักจับบัญชีอีเมลทหาร - หลอกลวงจิตวิทยา (Phishing) ส่งอีเมลหรือเอกสารราชการปลอม (Spear-Phishing) เพื่อหลอกให้เจ้าหน้าที่คลิกลิงก์อันตรายหรือฝัง Malware - ยิงระบบล่ม (DDoS): ระดมส่งทราฟฟิกมหาศาลถล่มเว็บไซต์กองทัพอากาศให้ใช้งานไม่ได้ เพื่อผลทางจิตวิทยาและดิสเครดิตองค์กร	๑๐
๑๓	การได้รับการสนับสนุนงบประมาณไม่เพียงพอ	การบริหารจัดการ RM03	- การขาดแคลนงบประมาณในการดำเนินการ เพื่อให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	๘
๑๔	นำข้อมูลของทางราชการไปใช้กับเทคโนโลยีปัญญาประดิษฐ์ (AI)	ผู้ปฏิบัติ RP04	- การใช้ AI (เช่น Generative AI หรือ Chatbot) สรุปรายงานราชการที่มีชั้นความลับ	๖
๑๕	การโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	การบริหารจัดการ/ผู้ปฏิบัติ RM04	- การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	๕

ลำดับ	ความเสี่ยง	ประเภท ความเสี่ยง	ลักษณะความเสี่ยง	ค่าระดับ ความเสี่ยง
๑๖	สถานการณ์ ความไม่สงบเรียบร้อย ในบ้านเมือง	ภัยพิบัติ หรือ สถานการณ์ฉุกเฉิน RE02	- การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	๒
๑๗	การเปลี่ยนแปลงนโยบาย ผู้บังคับบัญชา	การบริหารจัดการ RM02	- การเปลี่ยนแปลงผู้บังคับบัญชา อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่าง ๆ ได้รับผลกระทบ	๑

๙. การจัดลำดับความเสี่ยง

รร.การบิน กำหนดความสนใจต่อความเสี่ยงที่เกิดขึ้นตามค่าความเสี่ยงที่ได้จากการประเมิน ดังนี้

ระดับความเสี่ยงระดับต่ำ มีค่า = ๑ - ๘
ระดับความเสี่ยงระดับปานกลาง มีค่า = ๙ - ๑๖
ระดับความเสี่ยงระดับสูง มีค่า = ๑๗ - ๒๔
ระดับความเสี่ยงระดับสูงมาก มีค่า = ๒๕

เพื่อไม่เป็นภาระในการดำเนินการ การเตรียมการของผู้ดูแลระบบสารสนเทศ หรือมีการใช้งบประมาณดำเนินการเกินความจำเป็นในการวางแผนรองรับความเสี่ยง คณะจัดทำแผนบริหารความเสี่ยงพิจารณาว่าระดับความเสี่ยงที่จำเป็นให้ความสนใจและต้องบริหารจัดการความเสี่ยงของ รร.การบิน คือ ความเสี่ยงที่มีระดับความเสี่ยงตั้งแต่ ๑๒ ขึ้นไป ส่วนความเสี่ยงในระดับที่ต่ำกว่า ซึ่งผลกระทบไม่สูงมากนักให้ผู้ดูแลระบบสารสนเทศของ รร.การบิน และผู้ใช้งานระบบสารสนเทศ พิจารณาแก้ไขและพิจารณาดำเนินการตามความเหมาะสมของขีดความสามารถของบุคลากรในหน่วยงาน ทั้งนี้การดำเนินการใดที่หน่วยไม่สามารถดำเนินการได้เองให้ประสานการปฏิบัติกับผู้รับผิดชอบระบบสารสนเทศของ รร.การบิน

สำหรับความเสี่ยงที่เกิดขึ้นใน รร.การบิน จัดเรียงลำดับความเสี่ยงและแนวทางการจัดการความเสี่ยง ตามตารางดังนี้

ลำดับ	ความเสี่ยง	ระดับ ความเสี่ยง	มาตรการจัดการ ความเสี่ยง	แนวทาง การจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลา ปฏิบัติ
๑	RT02 การถูกบุกรุกโดยผู้ไม่ประสงค์ดี	๒๕	- จำกัดความเสี่ยง (มีแผนควบคุมความเสี่ยง)	๑. นทสส.รร.การบิน และกำลังพล รร.การบิน ตรวจสอบการตั้งค่าของ firewall ของเครื่องคอมพิวเตอร์และอุปกรณ์สารสนเทศ ๒. นทสส.รร.การบิน ติดตั้งระบบตรวจสอบการบุกรุก (Antivirus) เครือข่าย และคอมพิวเตอร์ทุกเครื่องใน รร.การบิน ๓. นทสส.รร.การบิน และ จนท.สารสนเทศ ของหน่วยติดตั้ง patch ของระบบปฏิบัติการตามวงรอบการอัพเดทของบริษัทเจ้าของลิขสิทธิ์	- คณก.รปภ.ระบบสารสนเทศฯ - นทสส.รร.การบิน	ทุก ๓ เดือน (ธ.ค. มี.ค. มิ.ย. ก.ย.)

ลำดับ	ความเสี่ยง	ระดับความเสี่ยง	มาตรการจัดการความเสี่ยง	แนวทางการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาปฏิบัติ
๒	RP03 ภัยคุกคาม Social Engineering การหลอกลวงโดยการทำ phishing และการกลั่นแกล้งรังแกบนโลกไซเบอร์ (Cyber bullying)	๒๕	จำกัดความเสี่ยง (มีแผนควบคุมความเสี่ยง)	๑. นทสส.รร.การบิน จัดทำมาตรการการใช้งานเครือข่ายคอมพิวเตอร์ ๒.จัดการอบรม หรือเผยแพร่ความรู้ให้ กำลังพล รร.การบิน และเพื่อให้รู้เท่าทันถึงภัยคุกคามทางไซเบอร์รูปแบบต่าง ๆ รวมทั้งแนะนำวิธีการรักษาข้อมูลส่วนตัวให้ปลอดภัย ๓. นทสส.รร.การบิน และ จนท.สารสนเทศฯ ประชาสัมพันธ์ให้กำลังพลทราบถึงภัยของการกลั่นแกล้งรังแกบนโลกไซเบอร์ โดยเฉพาะการโพสต์สิ่งที่ไม่ดีหรือทำลายชื่อเสียงของคนอื่นหรือ หน่วยงานของ ทอ.	- คณก.รปภ.ระบบสารสนเทศฯ - นทสส.รร.การบิน - กำลังพล รร.การบิน	ทุก ๓ เดือน (ต.ค. ม.ค. เม.ย. ก.ค.)
๓	RT02 การใช้ BYOD/Mobile Devices ใน รร.การบิน	๒๐	จำกัดความเสี่ยง (มีแผนควบคุมความเสี่ยง)	๑. จัดทำทะเบียนอุปกรณ์ BYOD/Mobile Devices ใน รร.การบิน ๒. ให้กำลังพลที่นำคอมพิวเตอร์ส่วนตัวมาใช้ในงานราชการมาลง Antivirus ที่ ทสส.ทอ.จัดหามาให้ ๓. ให้ความรู้และให้หลีกเลี่ยงการเชื่อมเครือข่ายสาธารณะเดือนละ ๑ ครั้ง	- คณก.รปภ.ระบบสารสนเทศฯ - นทสส.รร.การบิน - กำลังพล รร.การบิน	ทุก มี.ค.
๔	RT03 เครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	๒๐	- จำกัดความเสี่ยง (มีแผนควบคุมความเสี่ยง)	๑. กำลังพล รร.การบิน ป้องกันสัตว์กัดแทะอุปกรณ์สารสนเทศ ๒. นทสส.รร.การบิน และกำลังพล รร.การบิน จัดหาเครื่องและอุปกรณ์สำรองเพื่อทดแทนชั่วคราวให้สามารถปฏิบัติงานได้ ๓. นทสส.รร.การบิน และกำลังพล รร.การบิน ตรวจสอบและจัดจ้างบำรุงรักษาเครื่องและอุปกรณ์สารสนเทศที่สำคัญต่อระบบเครือข่ายตามวงรอบของการซ่อมบำรุงอุปกรณ์แต่ละชนิด	- คณก.รปภ.ระบบสารสนเทศฯ - นทสส.รร.การบิน - ผสอ.รร.การบิน	ทุก ก.ค.

ลำดับ	ความเสี่ยง	ระดับความเสี่ยง	มาตรการจัดการความเสี่ยง	แนวทางการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาปฏิบัติ
๕	RT04 การขาดแคนเครื่องคอมพิวเตอร์สำหรับการปฏิบัติงาน	๒๐	- จำกัดความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดทำโครงการขอคอมพิวเตอร์ในโครงการพัฒนาศักยภาพด้านเทคโนโลยีอย่างต่อเนื่องล่วงหน้า ๒ ปี - ให้ นขต.รร.การบิน ดำเนินการขอคอมพิวเตอร์จากโครงการแจกจ่ายครุภัณฑ์ประจำปีสายสื่อสาร ผ่าน นกบ.รร.การบิน และ ฝคก.รร.การบิน	- นกบ.รร.การบิน - นทสส.รร.การบิน - ผสอ.รร.การบิน - กรก.รร.การบิน	ช่วงเดือน พ.ค. - มิ.ย.
๖	RT07 การเชื่อมต่อระหว่างเครือข่ายภายนอกและเครือข่ายภายในไม่มีการรักษาความปลอดภัยผ่านระบบ NAC และ Firewall	๒๐	- ยอมรับความเสี่ยง เนื่องจากงบประมาณไม่เพียงพอ	- แจ้ง ทสส.ทอ.เพื่อขอรับการสนับสนุนการติดตั้ง Firewall เครือข่ายภายนอกโดยให้เหตุผลการเป็นเครือข่ายสำรองที่ใช้งานยุทธการ - แจ้งผู้ใช้งานเครือข่ายยุทธการให้แยกการใช้งานเครื่องคอมพิวเตอร์โดยห้ามเชื่อมต่อกับเครือข่ายภายนอก	- นทสส.รร.การบิน	เดือน ต.ค. และ เม.ย.
๗	RP02 การนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	๑๖	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	๑. นทสส.รร.การบิน จัดการฝึกอบรมเพื่อสร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยระบบสารสนเทศ ๒. นทสส.รร.การบิน และ จนท.สารสนเทศของหน่วยกระตุ้นให้เกิดการปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างจริงจัง ๓. ผสอ.รร.การบิน ใช้อุปกรณ์เครือข่ายที่สามารถจำกัดสิทธิ์การเข้าถึงสำหรับอุปกรณ์ที่ไม่ได้รับอนุญาตให้เชื่อมต่อเข้าเครือข่าย	- คณก.รปภ.ระบบสารสนเทศฯ - นทสส.รร.การบิน	ต.ค. และ ม.ค.ของทุกปีหรือตามโอกาส
๘	RP01 การเข้าถึงข้อมูลของบุคคลอื่น	๑๕	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	๑. นทสส.รร.การบิน สร้างความตระหนักรู้ในเรื่องของข้อมูลส่วนบุคคล ในการพึงรักษาสิทธิ์ของข้อมูลส่วนบุคคลตลอดเวลาหรือเมื่อมีโอกาส ๒. กำลังพล รร.การบิน เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ	- คณก.รปภ.ระบบสารสนเทศฯ - นทสส.รร.การบิน	ทุก ๖ เดือน ต.ค. เม.ย.

ลำดับ	ความเสี่ยง	ระดับความเสี่ยง	มาตรการจัดการความเสี่ยง	แนวทางการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาปฏิบัติ
๙	RT05 ระบบปฏิบัติการของเครื่องคอมพิวเตอร์ไม่สามารถอัพเดทได้	๑๕	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	๑. นทสส.รร.การบิน ดำเนินการ ตรวจสอบเครื่องคอมพิวเตอร์ทั้งหมดของ รร.การบิน เพื่อจัดทำฐานข้อมูลระบบปฏิบัติการของเครื่องคอมพิวเตอร์ ๒. ขออนุมัติ ผบช.ฯ เพื่อนำเครื่องคอมพิวเตอร์มาตรวจสอบและลงระบบปฏิบัติการใหม่ หากลงระบบปฏิบัติการใหม่ไม่ได้ให้ดำเนินการแก้ไขช่องโหว่และปิดช่องโหว่ หรือใช้ระบบปิดไม่เชื่อมต่อ อินเตอร์เน็ตตามคำแนะนำของ ศชบ.ทอ.	นทสส.รร.การบิน	ทุก ๖ เดือน ต.ค. และ เม.ย.
๑๐	RE01 กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	๑๒	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	๑. นขต.รร.การบิน จัดหาเครื่องกำเนิดไฟฟ้า และเครื่องสำรองไฟฟ้า ติดตั้งให้กับเครื่องคอมพิวเตอร์อุปกรณ์สารสนเทศที่มีความสำคัญต่อการใช้งาน เพื่อป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ ๒. ให้กำลังพล รร.การบิน ทำการบันทึกงานเอกสารทุก ๑๕ นาที ๓. กำลังพล รร.การบิน สำรองไฟล์งานเอกสารไว้ที่อุปกรณ์เก็บข้อมูลหรือ ฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์อื่นอย่างน้อยสัปดาห์ละ ๑ ครั้ง	- คณก.รปภ.ระบบสารสนเทศฯ - นทสส.รร.การบิน	ทุกเดือน ก.ย.
๑๑	RM01 การขาดแคลนบุคลากรผู้ปฏิบัติงาน	๑๒	- ยอมรับความเสี่ยง (มีมาตรการติดตาม)	๑. นทสส.รร.การบิน จัดทำคำสั่ง แต่งตั้งคณะทำงาน จนท.เทคโนโลยีสารสนเทศ นขต.รร.การบิน เพื่อให้มีเครือข่ายบุคคลากรด้านเทคโนโลยีสารสนเทศเพิ่มขึ้น ๒. นทสส.รร.การบิน จัดอบรมเจ้าหน้าที่สารสนเทศให้มีความรู้เพิ่มเติมอย่างน้อยปีละ ๒ ครั้ง ๓. นทสส.รร.การบิน จัดทำคู่มือกระบวนการทำงานเพื่อให้ จนท.สารสนเทศของ	- คณก.รปภ.ระบบสารสนเทศฯ - นทสส.รร.การบิน	ทุกเดือน ต.ค.

ลำดับ	ความเสี่ยง	ระดับความเสี่ยง	มาตรการจัดการความเสี่ยง	แนวทางการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาปฏิบัติ
				นขต.รร.การบิน สามารถปฏิบัติตามคู่มือได้ กรณีที่ นทสส.รร.การบิน หรือผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ ให้มีความรู้เพิ่มเติม - จัดทำคู่มือกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้ กรณีที่บุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้		
๑๒	RT06 การถูกโจมตีทางไ.เบอร์จากสถานการณ์ความตึงเครียดบริเวณชายแดนไทย-กัมพูชา	๑๐	-ยอมรับความเสี่ยง	๑.จัดชุดปฏิบัติการทางไซเบอร์ ๒.จัด จนท.เวรไซเบอร์ เพื่อเฝ้าระวังการถูกโจมตี เพื่อให้ทันต่อการติดต่อประสานจาก ศชบ.ทอ.เมื่อเกิดเหตุถูกโจมตี	- นทสส.รร.การบิน	ทุกวัน
๑๓	RM03 การได้รับการสนับสนุนงบประมาณไม่เพียงพอ	๘	-ยอมรับความเสี่ยง	- จัดทำโครงการเพื่อขอรับการสนับสนุน	- คณก.รปภ.ระบบสารสนเทศฯ - นทสส.รร.การบิน	ทุกเดือน มี.ค.
๑๔	RM04 การโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	๕	-ยอมรับความเสี่ยง	- ตรวจสอบการเข้าออกของบุคคลภายนอก - กำหนดพื้นที่หวงห้ามในการเข้าถึงพื้นที่ปฏิบัติงาน - ตรวจสอบระบบการป้องกันรักษาความปลอดภัยของสถานที่ให้อยู่ในสภาพปกติ - ติดตั้งกล้องวงจรปิดเพื่อเฝ้าระวัง	- คณก.รปภ.ระบบสารสนเทศฯ - นทสส.รร.การบิน	ทุกวัน
๑๕	RP04 นำข้อมูลของทางราชการไปใช้กับเทคโนโลยีปัญญาประดิษฐ์ (AI)	๖	-ยอมรับความเสี่ยง	จัดอบรมให้ความรู้กำลังพลของ รร.การบิน เกี่ยวกับการใช้ AI ที่ถูกต้องปลอดภัย	- นทสส.รร.การบิน	ทุก ๖ เดือน ต.ค.และ เม.ย.
๑๖	RE02 สถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	๒	- ยอมรับความเสี่ยง	- จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้	- คณก.รปภ.ระบบสารสนเทศฯ - นทสส.รร.การบิน	ตามสถานการณ์
๑๗	RM02 การเปลี่ยนแปลงนโยบายผู้บังคับบัญชา	๑	- ยอมรับความเสี่ยง	- ประชุมชี้แจงช่วงการปฏิบัติงานที่ผ่านมาให้ ผบช.ที่มารับตำแหน่งใหม่ได้เข้าใจ	- นทสส.รร.การบิน	ทุก ๖ เดือน ต.ค. และ เม.ย.

๑๐. บทสรุป...

๑๐. บทสรุปแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร รร.การบิน

การบริหารจัดการความเสี่ยง เป็นการป้องกันหรือลดผลกระทบจากความเสี่ยงที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งมีความแตกต่างกันไปตามสภาพแวดล้อม ภารกิจ เทคโนโลยีและระบบสารสนเทศที่แต่ละหน่วยมีใช้งาน การระบุความเสี่ยง ผลกระทบ และการพิจารณาแนวทางการบริหารจัดการความเสี่ยง ผู้รับผิดชอบระบบสารสนเทศของแต่ละหน่วยได้ร่วมระดมความคิดและพิจารณาจากประสบการณ์ และปัญหาที่แต่ละหน่วยเผชิญ โดยได้รวบรวมความเสี่ยง ผลกระทบ แนวทางในการบรรเทาผลกระทบหรือป้องกันไว้ในแผนบริหารความเสี่ยงนี้

แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ รร.การบิน ฉบับนี้ ได้ผ่านการพิจารณาจากคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ รร.การบิน เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการเพื่อจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร รร.การบิน ต่อไป

น.อ.
(คมกฤช เพชรสุข)
เสนาธิการ รร.การบิน/ผู้บริหารเทคโนโลยีสารสนเทศ (CIO)
ประธานคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ รร.การบิน
๑๖. มิ.ย.๖๙